

538,527

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2004 年 6 月 24 日 (24.06.2004)

PCT

(10) 国際公開番号  
WO 2004/054185 A1

- (51) 国際特許分類: H04L 12/56, 12/22
- (21) 国際出願番号: PCT/JP2002/012943
- (22) 国際出願日: 2002 年 12 月 11 日 (11.12.2002)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 三井物産株式会社 (MITSUI & CO., LTD.) [JP/JP]; 〒100-0004 東京都千代田区大手町一丁目2番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 大島 俊一 (OSHIMA, Shunichi) [JP/JP]; 〒100-0004 東京都千代田区大手町一丁目2番1号 三井物産株式会社内 Tokyo (JP). 斎藤 晃 (SAITO, Hikaru) [JP/JP]; 〒100-0004 東京都千代田区大手町一丁目2番1号 三井物産株式会社内 Tokyo (JP). 奈良原 智明 (NARAHARA, Tomoaki) [JP/JP]; 〒100-0004 東京都千代田区大手町一丁目

2 番 1 号 三井物産株式会社内 Tokyo (JP). 中里 昇吾 (NAKAZATO, Shogo) [JP/JP]; 〒100-0004 東京都千代田区大手町一丁目2番1号 三井物産株式会社内 Tokyo (JP). 吉川 治宏 (KIKKAWA, Haruhiro) [JP/JP]; 〒101-0052 東京都千代田区神田小川町 3-3-2 マツシタビル 三井物産デジタル株式会社内 Tokyo (JP). 荻猛 (OGI, Takeshi) [JP/JP]; 〒101-0052 東京都千代田区神田小川町 3-3-2 マツシタビル 三井物産デジタル株式会社内 Tokyo (JP).

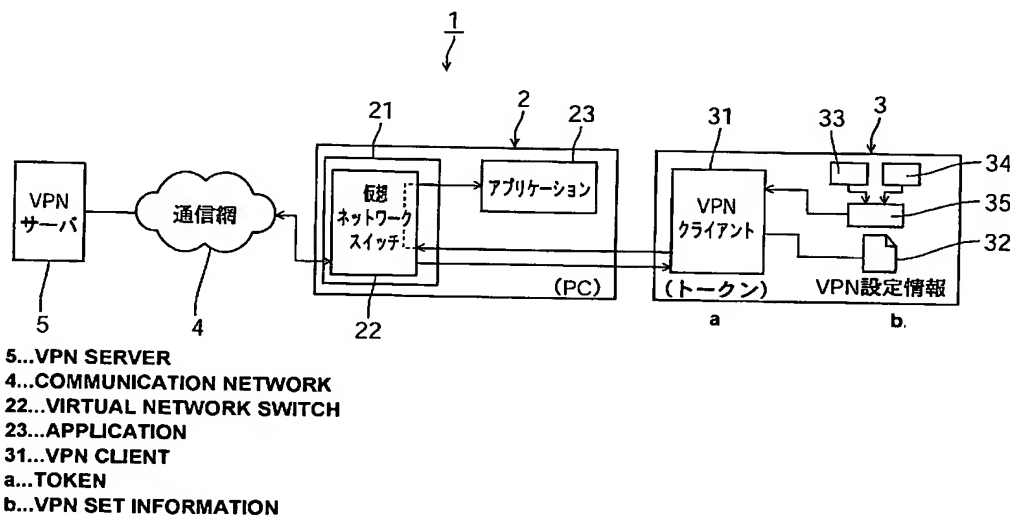
(74) 代理人: 市原 俊一, 外 (ICHIHARA, Shunichi et al.); 〒160-0004 東京都新宿区四谷2丁目8番地 コーポクロバ浜 505号 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SI, SK,

[続葉有]

(54) Title: COMMUNICATION SYSTEM, COMMUNICATION TERMINAL COMPRISING VIRTUAL NETWORK SWITCH AND PORTABLE ELECTRONIC DEVICE COMPRISING ORGANISM RECOGNITION UNIT

(54) 発明の名称: 通信システム、仮想ネットワークスイッチを備えた通信端末および生体認識装置を備えた携帯型電子デバイス



(57) Abstract: The communication terminal (2) of a communication system (1) comprises a virtual network switch (22) which can alter the destination of data being transmitted/received between the communication terminal (2) and a network (5) forcibly, wherein data is transmitted/received between the network (5) and the communication terminal (2) through a portable electronic device (3). Various functions, including a security function, can be supplemented by providing the function of software mounted on the portable electronic device (3) itself to the communication terminal (2). Even if a communication terminal connected directly with the network is not provided with such functions as VPN, firewall or virus check, high-safety communication can be ensured utilizing these security ensuring means mounted on the portable electronic device.

[続葉有]

WO 2004/054185 A1



SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN,  
YU, ZA, ZM, ZW.

許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR,  
NE, SN, TD, TG).

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW,  
MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許  
(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ  
特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,  
GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI 特

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される  
各PCTガゼットの巻頭に掲載されている「コードと略語  
のガイダンスノート」を参照。

---

(57) 要約:

通信システム (1) の通信端末 (2) は、ネットワーク (5) との間で  
送受されるデータの転送先を強制的に変更可能な仮想ネットワークスイ  
ッチ (22) を備え、ネットワーク (5) と通信端末 (2) の間のデー  
タの送受が、携帯型電子デバイス (3) を介して行われる。携帯型電子  
デバイス (3) 自身に搭載されているソフトウェアの機能を、通信端末  
(2) に提供し、セキュリティ機能などの各種の機能を補完することが  
できる。従って、ネットワークに直接接続される通信端末に、VPN、  
ファイアウォール、ウィルスチェックなどの機能が備わっていない場合  
においても、携帯型電子デバイスに搭載されているこれらのセキュリテ  
ィ確保手段を利用して、安全性の高い通信を行うことができる。

## 明細書

通信システム、仮想ネットワークスイッチを備えた通信端末および生体認識装置を備えた携帯型電子デバイス

5

## 技術分野

本発明は、ネットワーク通信機能を備えた通信端末および、当該通信端末との間で通信可能な携帯型電子デバイスを有する通信システムに関するものである。さらに詳しくは、携帯型電子デバイスに予め設定されている通信セキュリティレベルにより、通信端末を利用して各種のネットワークにアクセス可能な通信システムに関するものである。

10

## 背景技術

従来、インターネットなどの公衆網へ通信機器を接続して通信を行う際に必要なソフトウェア及びその設定情報などは、全て当該通信機器内部に予め搭載するか、もしくは当該通信機器に一時的にインストールさせて当該通信機器内部で同ソフトウェアを作動させる形式が一般的である。通信中のセキュリティを確保する場合にも、通信機器にセキュリティ確保用のソフトウェアを予め搭載するか、一時的にインストールするようになっている。

15

20

ここで、通信中のセキュリティを確保する手段として、通信する相手先との間で、規定の暗号化されたデータを使うことにより仮想専用線として共有回線の一部を利用してセキュリティを確保するVPN技術、通信中に不要な通信相手との情報交換を防ぐためのファイアウォール技術、交換したデータに対して悪意のあるウィルスソフトウェアが紛れ込んでいないかどうかを確認し、除去するための不正ウィルス除去技術などがある。

25

V P N技術については、インターネット上において通信を行う場合、不特定多数の他人によってデータが盗聴、改竄される危険を防止するために、I P - V P N技術が広く用いられている。I P - V P N技術を使う場合、通信を行うクライアント端末は、予め指定されたV P Nクライアント・ソフトウェアを通信端末内にインストールし、ネットワーク技術者が必要な設定作業を行うことにより、指定されたV P Nゲートウェイ装置との接続が可能となる。クライアント端末が相手先と通信する際、V P Nゲートウェイ装置を介して、暗号化された通信を行うことにより、インターネット上で相手先と安全に通信を実行することが出来る。

- 10 また、ファイアウォール技術については、予め通信端末上でO Sに標準搭載されているソフトウェアを用いて簡単な設定を施すことも出来る。しかし、企業内などで使用する場合には、ファイアウォールソフトウェアを購入し各通信端末に導入するか、あるいは、専用のファイアウォール装置を購入し、ネットワークの入口部分に設置して、ネットワーク自体を予め防御してしまう方法などが一般的である。いずれも、一般的には専門家による事前の設定作業が必要であり、従って特定の端末、特定のネットワークを対象とした防御方法となるのが通常である。

- さらに、不正ウィルス除去技術についても、上記ファイアウォール技術同様、予めウィルス除去ソフトウェアを通信端末上に導入して定期的に除去作業を行うか、あるいはネットワーク上の特定のサーバ装置などに同ウィルス除去ソフトウェアを導入し、同装置経由で通信を行うことにより、サーバ上でウィルスを駆除してしまうものなどが一般的である。

- 従来の技術においては、通信の開始にあたり、ネットワーク機器に予め必要なソフトウェアが全て搭載されていることを前提としていることが多い。しかしながら、現在の社会においてはインターネットを代表とするネットワークへの接続の手段は無数にあり、予めネットワークの管理責任者の管理下で制御されたネットワーク機器を介さずとも、個人が

自分の意志で自由にネットワークを活用することが出来、ネットワーク管理者による限定的なエリアでのネットワーク制御、情報制御は事実上何の意味も持っていないのが現状であり、ネットワークにアクセスを試みる個人自身に対してネットワークの管理手段を提供することが急務である。昨今、インターネットカフェや公衆無線サービスが提供されているが、これらの回線、端末を運用管理する企業がどの程度のセキュリティに対する防御策をとっているかを知る事は難しく、自身が操作する通信端末は自らの防御策を持って利用することが望ましいと考える。

一方、通信端末自身の処理能力の観点からも次のような弊害が生じている。すなわち、年々個々の通信端末に搭載されるソフトウェア・ハードウェアの必要処理能力は拡大の一途をたどっており、それに合わせて通信端末の処理能力も確実に上昇している。しかしながら、通信端末の処理能力が向上しているとはいえ、あらゆる業務を一つの通信端末が全て処理する場合には、当該通信端末が遂行すべきユーザに対するアプリケーション実行能力を制限して、通信に関わる業務を実行しなければならない場合が生ずる。

ネットワークの高速化に伴う情報量の増大により、それによる被害は更に頻発する傾向にある。また、ユーザの観点から見た場合、そのような一部の作業の遅延による障害が発生することを理由として、通信端末そのものを買い換える必要性が生じてしまうので、効率が悪い。また、複数の通信端末を利用して通信を行うようなユーザの場合、個々の端末の能力に通信環境の状態を依存させることとなり、ネットワーク品質が不安定になることが避けられない。

個々のセキュリティ技術、例えば、VPN技術を用いた通信を行う場合には、前提としてクライアント端末に対してVPNクライアント・ソフトウェアがインストールされており、必要な通信用の設定が既になされている必要がある。また、この通信用の設定は一般的にはネットワー

ク技術に詳しく、かつ通信先のVPNゲートウェイが必要とする設定情報を全て知らない限り、設定することは困難である。

この結果、VPNの通信を行える端末は、予め企業が従業員に設定済みの状態で配布する情報端末に限定される。当該情報端末を従業員が持  
5 参しない限り、企業のリソースに対してVPN接続による通信を行うことは事実上不可能である。その対策として、そのような従業員は、一般公衆回線を用いた低速のダイヤルアップ接続を行うか、あるいは企業の管理者のセキュリティ管理が及ばない第三者のインターネット事業者、携帯電話事業者などが提供するサービスを利用して限定されたメールに  
10 アクセスする、などしかない。しかし、本来このような方法はネットワーク管理者としては危険な状況であり、好ましくない。

また、VPNクライアント・ソフトウェア上に設定された通信用の各種設定情報については、簡単なセキュリティ・チェックを通過すれば、通信端末の所有者以外の第三者が簡単にアクセスすることが可能である。  
15 従って、悪意のある第三者が不注意なクライアント端末所有者の端末から、比較的容易に設定情報を盗み出し、別の端末上に設定してVPNゲートウェイと接続することによって、企業などの秘密データへアクセスすることが出来てしまう難点がある。

その他ファイアウォールの利用、ウィルス除去ソフトウェアの利用などに当っては、従来の技術では利用できるネットワーク、通信端末に限りがあり、広く一般的なインターネットを、実際に通信を行う通信端末自体に限定されずに安心して利用する手段がないのが現状である。  
20

#### 発明の開示

25 本発明の目的は、上記の点に鑑みて、通信機能を備えた通信端末に予め必要なソフトウェアが全て搭載されていることを前提とせずに、当該通信端末を用いて、希望するセキュリティレベルでの通信を行うことを

可能にする通信システム、並びに当該通信システムに用いるための通信端末および携帯型電子デバイスを提案することにある。

上記の目的を達成するために、本発明の通信システムは、  
ネットワーク接続手段を備えた通信端末と、

- 5 当該通信端末との間で通信が可能な携帯型電子デバイスとを有し、  
前記通信端末は、前記ネットワーク接続手段によって接続されたネットワークとの間で送受されるデータの転送先を強制的に変更可能な仮想ネットワークスイッチを備えており、

- 前記携帯型電子デバイスは、前記通信端末による前記ネットワークとの間の通信セキュリティを確保するためのセキュリティ確保手段を備えており、

前記通信端末は、前記仮想ネットワークスイッチおよび前記携帯型電子デバイスの前記セキュリティ確保手段を介して、前記ネットワークとの間でデータの送受を行うことを特徴としている。

- 15 ここで、前記セキュリティ確保手段としては、VPN手段、ウィルス除去手段、およびファイアウォール手段を挙げることができる。

- また、前記仮想ネットワークスイッチは、インターネット標準プロトコルであるTCP/IPにおけるOSI 7階層モデルのネットワーク層に組み込まれた仮想IPスイッチとすることができる。この仮想IPス
- 20 イッチは、前記ネットワークから受け取ったパケットを、予め設定されている条件に従って、上位のトランスポート層あるいは前記携帯型電子デバイスに転送し、当該携帯型電子デバイスからのパケットを、予め設定されている条件に従って、上位のトランスポート層あるいは送信元の前記ネットワークに戻すことを特徴としている。

- 25 次に、本発明の通信システムは、上記構成に加えて、前記通信端末の記憶媒体、およびアプリケーションのセキュリティのチェックを、前記仮想ネットワークスイッチを介して、前記携帯型電子デバイスの前記セ

セキュリティ確保手段により行うことを特徴としている。

また、前記携帯型電子デバイスは、指紋センサなどの生体認識装置と、予め生体情報が記憶保持された生体情報記憶部と、前記生体認識装置により読み取られた生体情報を前記生体情報記憶部に記憶されている生体  
5 情報と照合することにより、前記通信端末を介しての前記ネットワークに対するアクセスを許可する認証手段とを備えていることが望ましい。

一方、本発明の通信システムは、

ネットワーク接続手段を備えた通信端末と、

当該通信端末との間で通信が可能な携帯型電子デバイスとを有し、

10 前記通信端末は、ネットワークとの間の通信セキュリティを確保するためのセキュリティ確保手段を備えており、

前記携帯型電子デバイスは、前記セキュリティ確保手段を介して前記ネットワークとの通信を行うために必要な通信設定情報を記憶保持した通信設定情報記憶部と、指紋センサなどの生体認識装置と、予め生体情  
15 報が記憶保持された生体情報記憶部と、前記生体認識装置により読み取られた生体情報を前記生体情報記憶部に記憶されている生体情報と照合する認証手段とを備えていることを特徴としている。

このように構成した本発明の通信システムにおいては、利用するネットワーク通信機能を有する通信端末に搭載されているソフトウェアの種  
20 類に限定されず、携帯型電子デバイス自身に搭載されているソフトウェアの機能を、当該通信端末に対して提供し、セキュリティ機能などの各種の機能を補完することができる。従って、ネットワークに直接接続される通信端末に、VPN、ファイアウォール、ウィルスチェックなどの機能が備わっていない場合においても、携帯型電子デバイスに搭載され  
25 ているこれらのセキュリティ確保手段を利用して、安全性の高い通信を行うことができる。

また、携帯型電子デバイスは自身が固有の物理的なネットワーク接続



手段を持たないが、ネットワークに直接接続された別の通信端末に接続すると、通信端末の仮想ネットワークスイッチによって、当該携帯型電子デバイスが、ネットワークと当該通信端末の間に仮想的に介在することになる。従って、携帯型電子デバイスに搭載されているセキュリティ

5 確保手段を利用して、通信端末とネットワークとの間で通信を行うことができる。

さらに、携帯型電子デバイスが生体認識装置を備えている場合には、当該生体認識装置によって本人認証を行うことにより、同デバイスが接続されたPC、携帯電話などの固有の物理的にネットワークに接続された通信端末を通じて、インターネット上の指定されたネットワークに対する接続を確立することができる。

10

#### 図面の簡単な説明

図1は、本発明を適用した通信システムの一例を示す全体構成図である。

15

図2は、本発明を適用した通信システムの別の例を示す全体構成図である。

図3は、本発明を適用した通信システムのさらに別の例を示す全体構成図である。

20 図4は、図1～図3の通信システムの通信端末に搭載されている仮想ネットワークスイッチの例を示す説明図である。

図5は、図1～図3の通信システムの通信端末に搭載されている仮想ネットワークスイッチの例を示す説明図である。

図6は、本発明の別の形態に係る通信システムの例を示す全体構成図である。

25

図7は、図6の通信システムの変形例を示す全体構成図である。

図8は、図6の通信システムの別の変形例を示す全体構成図である。

発明を実施するための最良の形態

以下に、図面を参照して本発明を適用した通信システムの実施例を説明する。

- 5 図 1 は、本発明を適用した通信システムの一例を示す全体構成図である。本例の通信システム 1 は、P C、携帯電話などのようなネットワーク接続手段 2 1 を備えた通信端末 2 と、当該通信端末 2 との間で通信が可能な携帯型電子デバイス 3（以下、「トークン」と呼ぶこともある。）とを有し、インターネットなどの通信網 4 を介して所定のネットワーク  
10 5 に接続可能となっている。

- 通信端末 2 は、ネットワーク接続手段 2 1 によって接続されたネットワーク 5 との間で送受されるデータの転送先を強制的に変更可能な仮想ネットワークスイッチ 2 2 を備えている。この仮想ネットワークスイッチ 2 2 により、ネットワーク 5 から通信端末 2 に送信されてきたデータ  
15 が携帯型電子デバイス 3 に転送され、当該携帯型電子デバイス 3 を経由して、再び通信端末 2 の仮想ネットワークスイッチ 2 2 に戻され、ここから通信端末 2 のアプリケーション 2 3 などによって処理されることになる。通信端末 2 からネットワーク 5 への送信データも仮想ネットワークスイッチ 2 2 から携帯型電子デバイス 3 を経由して再び仮想ネットワーク  
20 スwitch 2 2 を介して通信先のネットワーク 5 に向けて送信される。このように、仮想ネットワークスイッチ 2 2 によって、携帯型電子デバイス 3 は、物理的には通信端末 2 に接続されているが、あたかも、ネットワーク 5 と通信端末 2 の間に介在しているかのように機能する。

- この携帯型電子デバイス 3 は、通信端末 2 によるネットワーク 5 との  
25 間の通信セキュリティを確保するためのセキュリティ確保手段を備えている。本例では、V P N クライアント機能 3 1 および V P N 設定情報が記憶された記憶部 3 2 を備えている。

従って、本例の通信システム 1 においては、携帯型電子デバイス 3 を通信端末 2 に接続して相互通信可能にした後に、通信端末 2 の通信接続手段 2 1 を用いてネットワーク 5 (VPNサーバ) との通信を開始すると、仮想ネットワークスイッチ 2 2 が機能する。この結果、携帯型電子デバイス 3 の VPN を利用した通信が、ネットワーク 5 と通信端末 3 の間に形成される。

ここで、携帯型電子デバイス 3 は、指紋センサなどの生体認識装置 3 3 と、予め生体情報が記憶保持された生体情報記憶部 3 4 と、生体認識装置 3 3 により読み取られた生体情報を生体情報記憶部 3 4 に記憶されている生体情報と照合することにより認証を行う認証部 3 5 を備えていることが望ましい。

図 2 は本発明による通信システムの別の例を示す全体構成図である。この図に示す通信システム 1 A は、仮想ネットワークスイッチ 2 2 による機能を利用して、通信端末 2 A の媒体 (ハードディスク、リムーバブルディスク、外付けのメモリなど) の管理や、プログラムの実行管理を、携帯型電子デバイス 3 A の側から行うように構成されている。

通信端末 2 A の仮想ネットワークスイッチ 2 2 は、当該通信端末 2 A の記憶媒体 (ハードディスクやリムーバブルディスク等) 2 4 にアクセスする機能を備えている。携帯型電子デバイス 3 A にはセキュリティ確保手段としてのウィルスチェック機能 3 1 A、ウィルスパターン情報記憶部 3 2 A が備わっている。

携帯型電子デバイス 3 A を通信端末 2 A に接続して、本人認証が行われた後は、ウィルスチェック機能 3 1 A は、通信端末 2 A の仮想ネットワークスイッチ 2 2 に対して、記憶媒体 2 4、アプリケーション 2 3 へアクセスするためのコマンドパケットを発行する。これにより、通信端末 2 A の各種媒体に対するセキュリティのチェックを携帯型電子デバイス 3 A の側から行うことができる。

図 3 は本発明による通信システムのさらに別の例を示す全体構成図である。この図に示す通信システム 1 B は、携帯型電子デバイス 3 B に、セキュリティ確保手段としてのファイアウォール機能 3 1 B と、そのためのファイアウォール設定情報の記憶部 3 2 B を設けた構成となっている。この通信システム 1 B においても、仮想ネットワークスイッチ 2 2 の機能によって、携帯型電子デバイス 3 B が、通信網 4 と通信端末 2 B の間に仮想的に介在して、外部からの不正侵入の検知を行うので、安全な通信を行うことができる。

ここで、通信端末 2 (2 A、2 B) に設けられている仮想ネットワークスイッチ 2 2 は、インターネット標準プロトコルである TCP / IP における OSI 7 階層モデルのネットワーク層に組み込まれた仮想 IP スイッチとすることができる。

図 4 は OSI の 7 階層モデルを示す説明図である。7 階層モデル 6 におけるネットワーク層 6 3 に仮想 IP スイッチ 6 8 がインストールされている。仮想 IP スイッチ 6 2 がパケットの転送先を上位トランスポート層 6 3 あるいは他のネットワーク機器である携帯型電子デバイス 3 (3 A、3 B) に切り替える。その他の各層 6 1、6 2、6 4 ~ 6 7 については何ら変更を加える必要がない。

仮想 IP スイッチ 6 8 は、一般的なレイヤー 3 のスイッチとは機構が異なり、パケットを携帯型電子デバイス 3 (3 A、3 B) に転送する場合には、元パケットの情報を欠落することなく維持する必要があるので、元パケットを転送用のパケットでカプセリングする必要がある。カプセル化されたパケットは、転送先のデバイス 3 (3 A、3 B) においてオリジナルのパケットに戻され、当該デバイス上のアプリケーションで処理が行われ、再度、仮想 IP スイッチ 6 8 に当該パケットが渡される。

なお、図 5 には、当該 7 階層モデルを、ウィンドウズ (登録商標) のネットワークモデルに当てはめた場合の説明図である。この図において、

インターミディエイト層 (Intermediate層) 上の「vsw.  
sys」が仮想ネットワークスイッチである。このソフトウェアが、携  
帯型電子デバイス 3 (3A、3B) および通信端末 2 (2A、2B) 上  
の上位プロトコルのいずれにパケットを転送するのかを決定する。この  
5 インターミディエイト層はウィンドウズのネットワークアーキテクチュ  
アに標準的に用意された層であり、この層を利用したパケットフィルタ  
リングのソフトウェアなどが市販されている。

次に、図 6 は、本発明による通信システムを示す全体構成図である。  
この通信システム 1C も、通信端末 2C と携帯型電子デバイス (トーク  
10 ン) 3C とを備えている。通信端末 2C はネットワーク通信手段 21A  
を備えていると共に、VPN クライアント機能 26 を備えている。これ  
に対して、携帯型電子デバイス 3C は、当該 VPN クライアント機能 2  
6 を用いて通信を行うために必要な VPN 設定情報が記憶された記憶部  
32C を備えている。また、携帯型電子デバイス 3C には、指紋センサ  
15 などの生体認識装置 33 と、予め生体情報が記憶保持された生体情報記  
憶部 34 と、生体認識装置 33 により読み取られた生体情報を生体情報  
記憶部 34 に記憶されている生体情報と照合することにより認証を行う  
認証部 35 が備わっている。

この構成の通信システム 1C では、セキュリティーを処理するプログ  
20 ラムを通信端末 2C の側に搭載し、それを稼動させるために必要な情報  
をトークン 3C の側に保持し、生体認識装置 33 による認識結果によっ  
てそれらが協調して処理が実行される。

図 7 は、本発明を適用したウィルスチェック機能を備えた通信システ  
ムを示す全体構成図である。この通信システム 1D では、通信端末 2D  
25 の側にウィルスチェック機能 (ソフトウェア) 27 が搭載され、それを  
実行するために必要なウィルス設定情報が携帯型電子デバイス 3D の記  
憶部 32D に保持されている。生体認識装置 33 により認証されると、

双方が協同してウィルスチェックを行い、安全な通信を行うことができる。

次に、図 8 は、本発明を適用したファイアウォール機能を備えた通信システムを示す全体構成図である。この通信システム 1 E では、通信端  
5 末 2 E の側にパーソナルファイアウォール機能 2 8 が搭載され、携帯型電子デバイス 3 E にはそのためのファイアウォール設定情報が記憶された記憶部 3 2 E が備わっている。この場合にも、生体認識装置 3 3 によって本人認証が行われると、双方が協同して、安全な通信を行うことができる。

10

#### 産業上の利用の可能性

以上説明したように、本発明の通信システム、それに用いる通信端末および携帯型電子デバイスによれば次のような効果が得られる。

(1) 本発明による生体認識装置付きの携帯型電子デバイスを持ち歩く  
15 ことにより、利用者は、あらゆる場所で、あらゆるネットワーク通信機能を有する通信端末を用いて、必要なインターネット上のリソースに対して V P N 接続やセキュリティーチェックを行いながら安全な通信を行うことが可能となる。従って、回線事業者により設定されているセキュリティー上の制約に囚われず、必要な場所で自ら設定したセキュリティー  
20 ポリシーを維持しながら、利用可能な最適な通信手段を用いて通信を行うことが可能となる。

(2) 通信端末にはセキュリティーを脅かす情報を保持する必要がなくなり、携帯型電子デバイスに V P N 接続やパーソナルファイアウォール設定、ウィルスチェック設定、その他セキュリティーに関する通信設定情  
25 報を暗号化して保存することにより、外部の第三者に対する設定情報の漏洩の危険性が格段に少なくなる。

(3) セキュリティーチェックのために費やされる通信端末の負荷が軽減

され、他の処理のパフォーマンス向上が期待できる。

(4) 上記の(2)に関連して、通常の使用にあたってユーザ自身がVPNクライアント・ソフトウェア等の操作に関わることは殆ど必要なくなる。また、設定情報へアクセスすることを、ネットワーク管理者のみ  
5 が利用可能な暗号化手段によって制限するなどの作業が可能になるので、不注意によってクライアント・ソフトウェアの設定情報を変更してしまう危険性も格段に少なくなる。結果として、ネットワーク管理者の労力、企業の管理コストの低減効果が見込まれる。

(5) 本発明の携帯型電子デバイスを個人がIDとして持ち歩き、ID  
10 と連携したVPNソフトウェア、パーソナルファイアウォール、ウィルス除去ソフトウェア、及びその接続に関する通信設定情報を保存することができる。このようにすれば、当該デバイスを貸し与える企業などは、ユーザである従業員の異動、利用するPCなどの通信機器の交換などに際して、新しく利用する通信機器へのVPNクライアント・ソフトウェア  
15 のインストール作業、VPN接続用の設定作業などを行う必要がなくなる。単に、当該トークンとの通信インターフェースを確保しておけばよいだけとなるので、ネットワーク管理者の労力が格段に低減される。

(6) 上記IDに関連し、本発明による仕組みをセキュリティーソフトウェア等のソフトウェアと関連させることにより、生体認識装置による  
20 本人認証、認証後のIDのネットワーク・サーバへの発行によるライセンス情報の確認、ライセンス確認後のトークンに内蔵されたソフトウェアのアップデート機能の提供などを、端末に対してではなく、それを持ち運ぶ本人に対して確実に実行することが可能となる

(7) 通信端末の仕様が、利用しているアプリケーションや通信ソフトウェアの機能を十分に提供できない場合、通信端末そのものを買換  
25 えることなく、必要な通信処理能力のみ、別の分散処理装置に置き換えることで対応出来るとともに、そのような分散処理装置を持ち運ぶことに

よって、端末自体を持ち運ぶことなく、常に安定した通信環境を得ることが可能となる。



## 請求の範囲

1.           ネットワーク接続手段を備えた通信端末と、

当該通信端末との間で通信が可能な携帯型電子デバイスとを有し、

5   前記通信端末は、前記ネットワーク接続手段によって接続されたネットワークとの間で送受されるデータの転送先を強制的に変更可能な仮想ネットワークスイッチを備えており、

前記携帯型電子デバイスは、前記通信端末による前記ネットワークとの間の通信セキュリティを確保するためのセキュリティ確保手段を備えており、

10 前記通信端末は、前記仮想ネットワークスイッチおよび前記携帯型電子デバイスの前記セキュリティ確保手段を介して、前記ネットワークとの間でデータの送受を行うことを特徴とする通信システム。

15 2.           請求の範囲第1項において、

前記セキュリティ確保手段は、少なくとも、VPN手段、ウィルス除去手段、およびファイアウォール手段のいずれか一つを含むことを特徴とする通信システム。

20 3.           請求の範囲第1項または第2項において、

前記仮想ネットワークスイッチは、インターネット標準プロトコルであるTCP/IPにおけるOSI 7階層モデルのネットワーク層に組み込まれた仮想IPスイッチであり、

25 当該仮想IPスイッチは、前記ネットワークから受け取ったパケットを、予め設定されている条件に従って、上位のトランスポート層あるいは前記携帯型電子デバイスに転送し、当該携帯型電子デバイスからのパケットを、予め設定されている条件に従って、上位のトランスポート層

あるいは送信元の前記ネットワークに戻すことを特徴とする通信システム。

4. 請求の範囲第1項、第2項または第3項において、

5 前記通信端末の記憶媒体、およびアプリケーションのセキュリティのチェックを、前記仮想ネットワークスイッチを介して、前記携帯型電子デバイスの前記セキュリティ確保手段により行うことを特徴とする通信システム。

10 5. 請求の範囲第1項ないし第4項のうちのいずれかの項において、

前記携帯型電子デバイスは、指紋センサなどの生体認識装置と、予め生体情報が記憶保持された生体情報記憶部と、前記生体認識装置により読み取られた生体情報を前記生体情報記憶部に記憶されている生体情報  
15 と照合することにより、前記通信端末を介しての前記ネットワークに対するアクセスを許可する認証手段とを備えていることを特徴とする通信システム。

6. 請求の範囲第1項ないし第5項のうちのいずれかの項に記載  
20 されている前記仮想ネットワークスイッチを備えた前記通信端末。

7. 請求の範囲第1項ないし第5項のうちのいずれかの項に記載されている前記携帯型電子デバイス。

25 8. ネットワーク接続手段を備えた通信端末と、  
当該通信端末との間で通信が可能な携帯型電子デバイスとを有し、  
前記通信端末は、ネットワークとの間の通信セキュリティを確保する

ためのセキュリティ確保手段を備えており、

前記携帯型電子デバイスは、前記セキュリティ確保手段を介して前記ネットワークとの通信を行うために必要な通信設定情報を記憶保持した通信設定情報記憶部と、指紋センサなどの生体認識装置と、予め生体情報5 報が記憶保持された生体情報記憶部と、前記生体認識装置により読み取られた生体情報を前記生体情報記憶部に記憶されている生体情報と照合する認証手段とを備えていることを特徴とする通信システム。

9. 請求の範囲第8項において、

10 前記セキュリティ確保手段は、少なくとも、VPN手段、ウィルス除去手段、およびファイアウォール手段のいずれか一つを含むことを特徴とする通信システム。

10. 請求の範囲第8項または第9項に記載されている前記携帯15 型電子デバイス。

図1

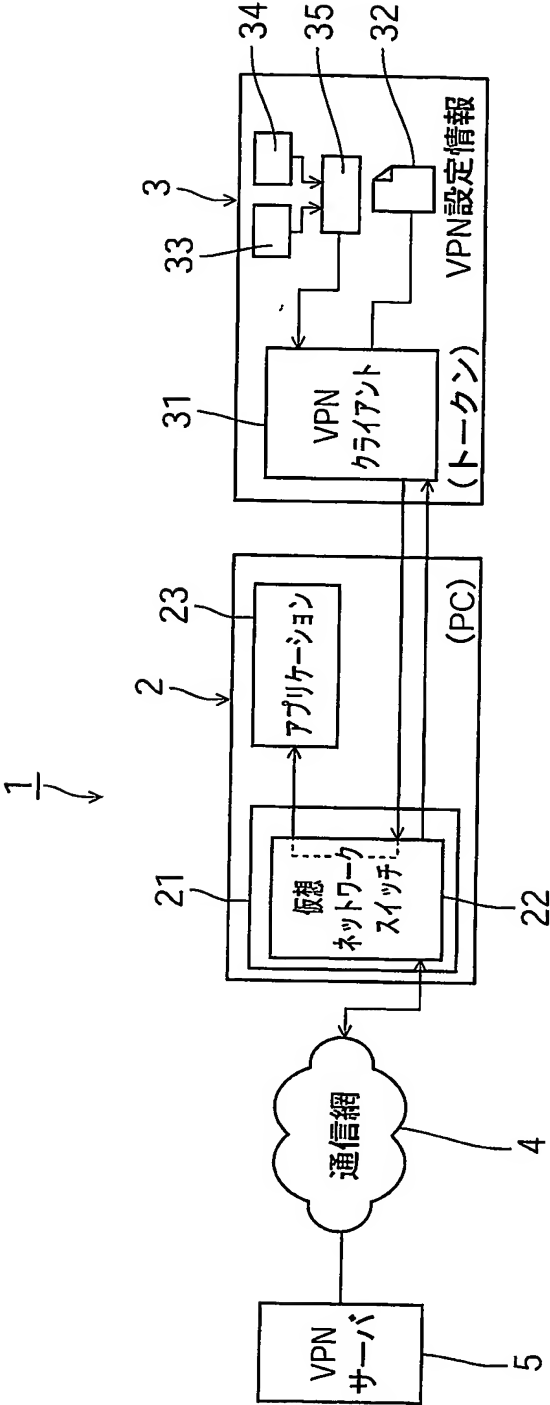


図2

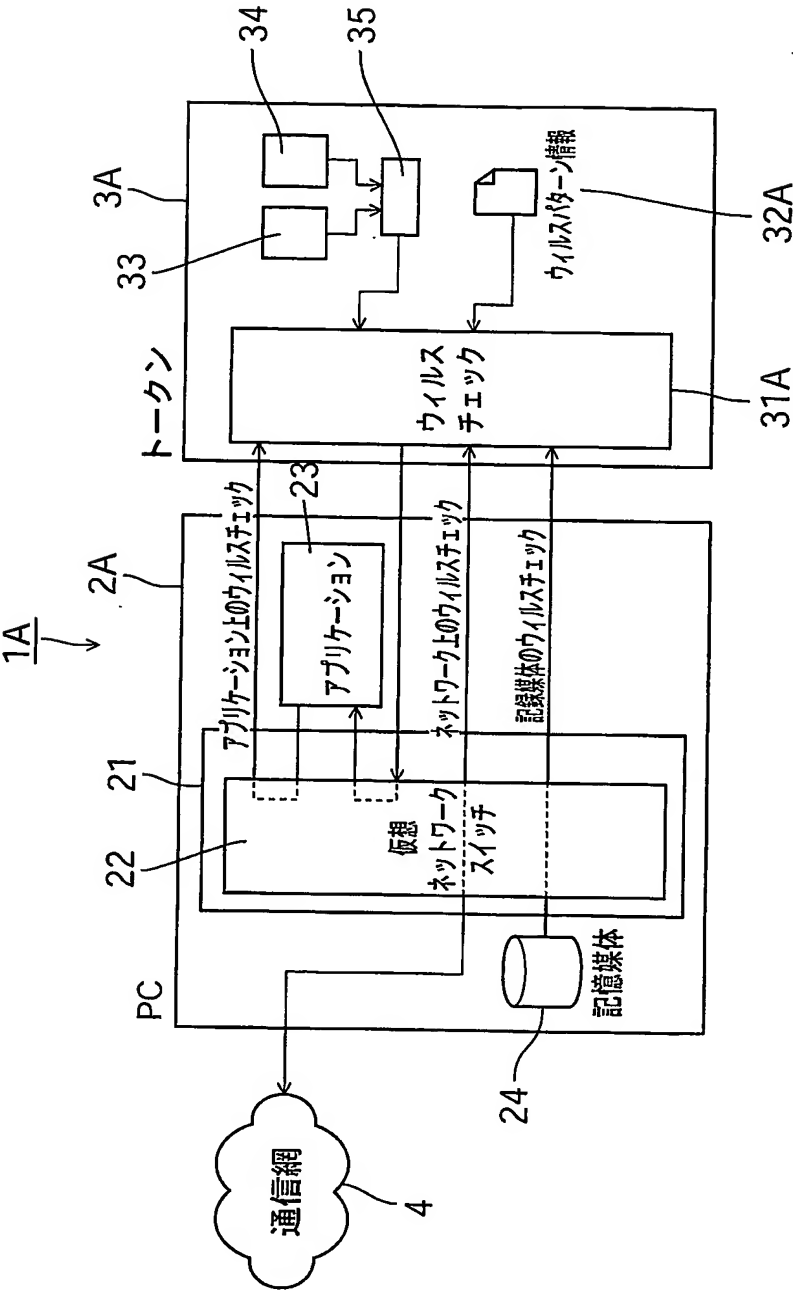
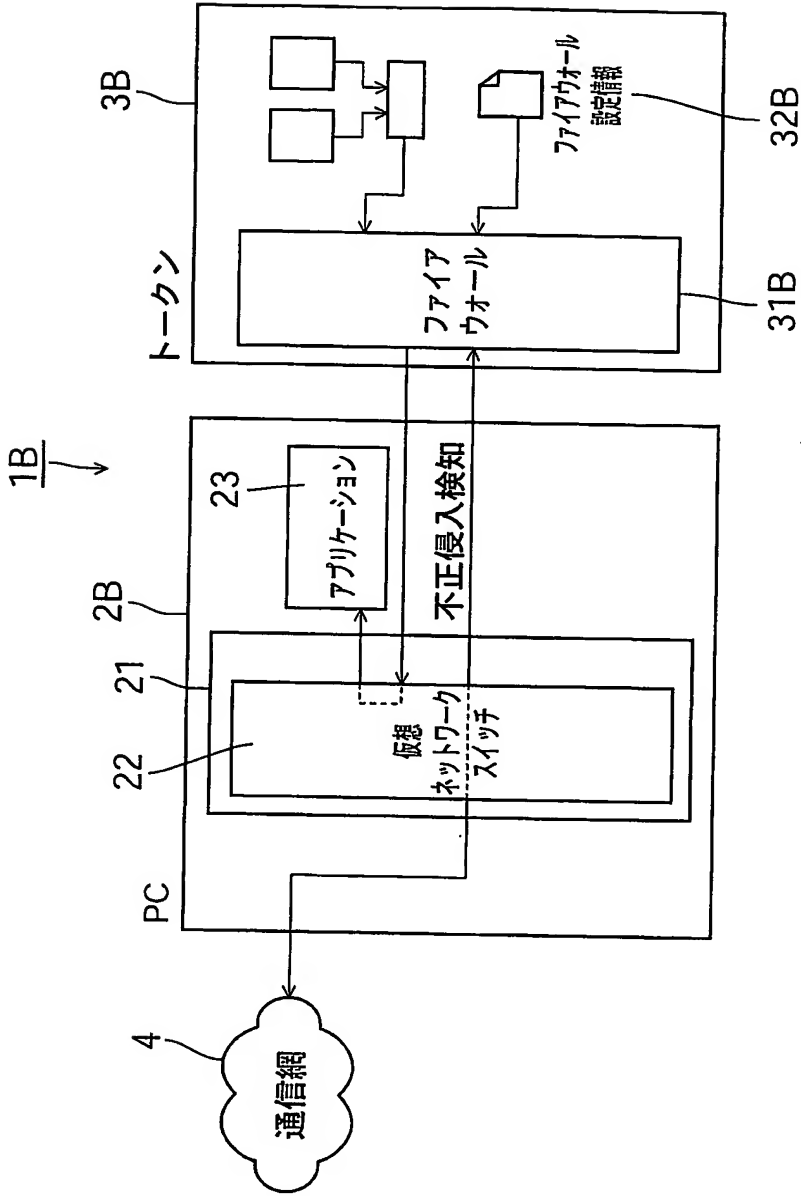


図3



4 / 8

図4

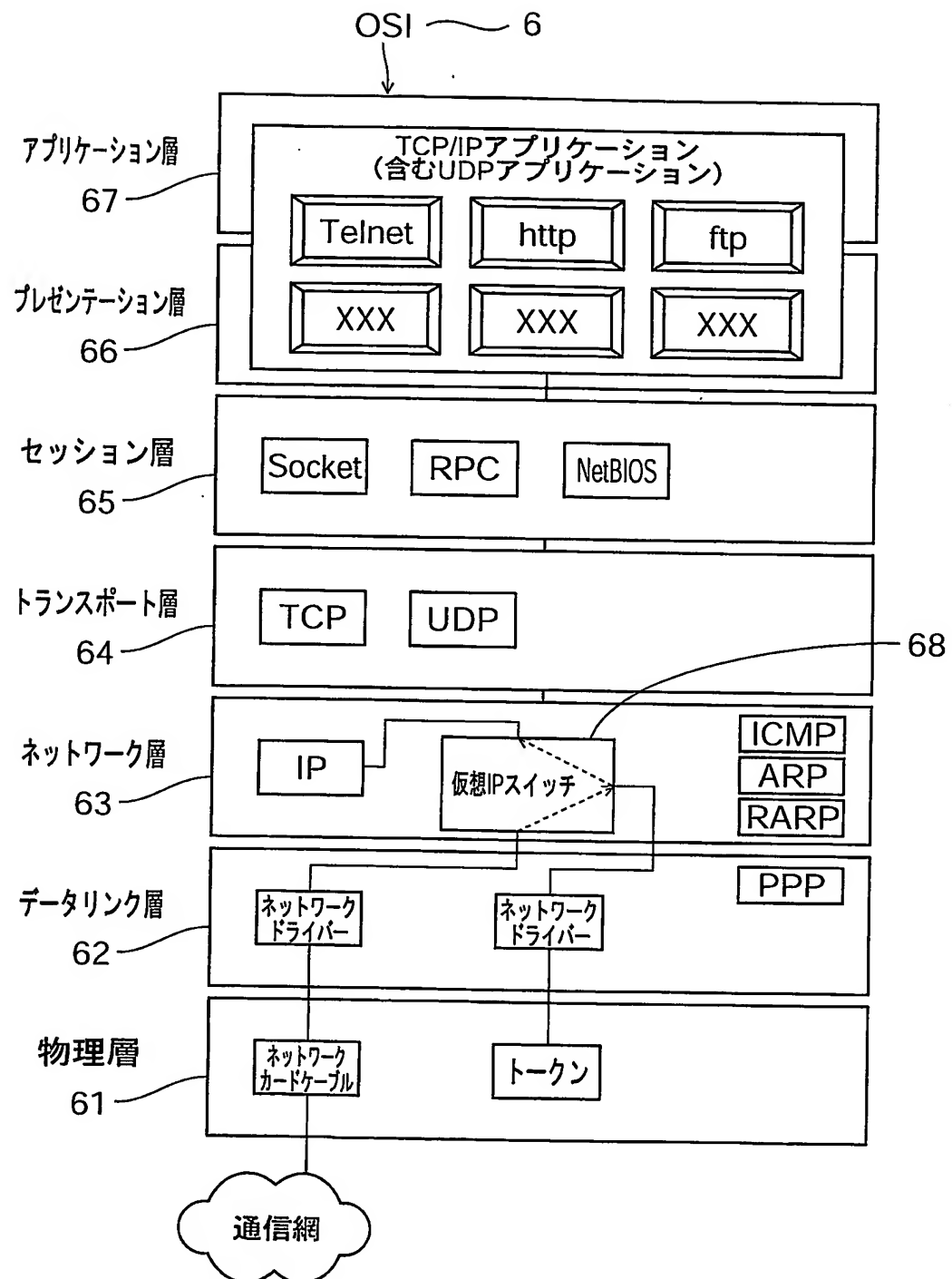


図5

## Windowsのネットワークモデル

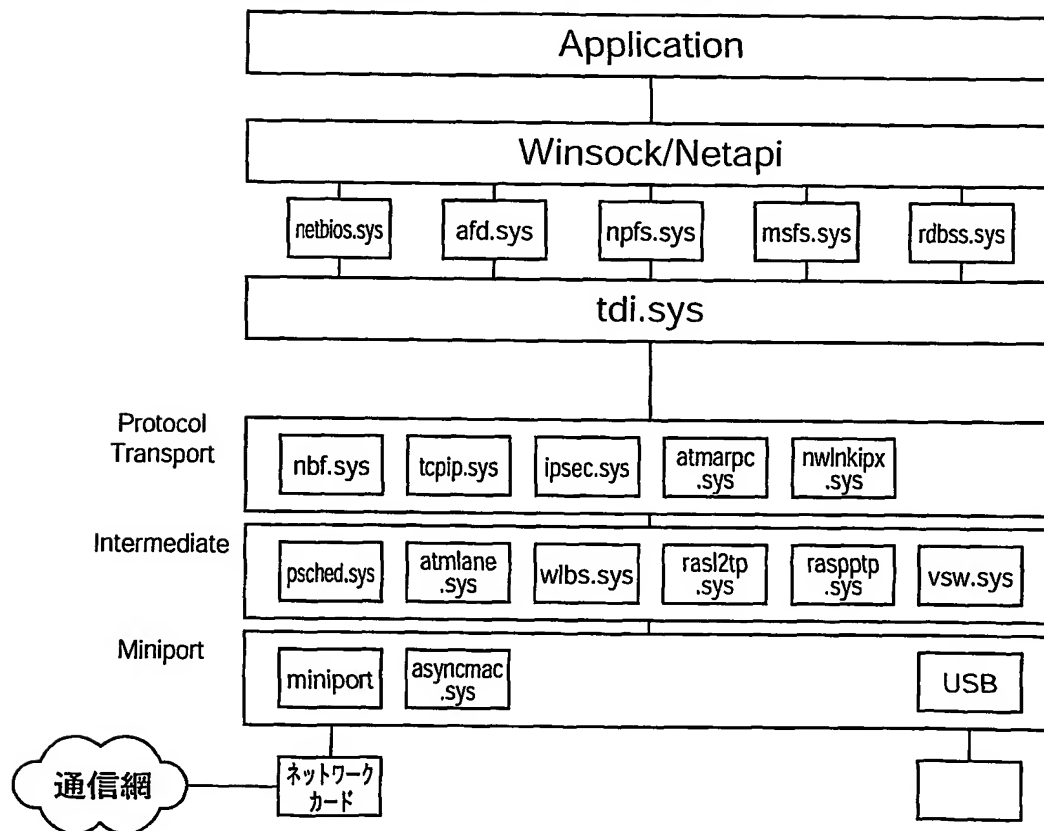




図6

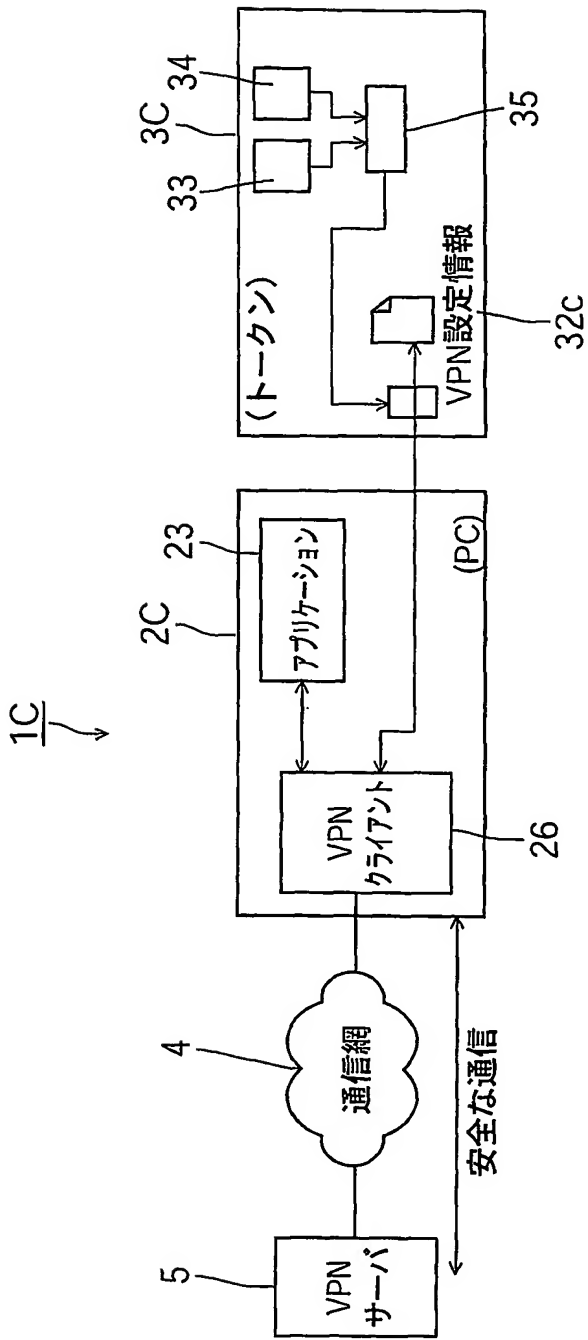


図7

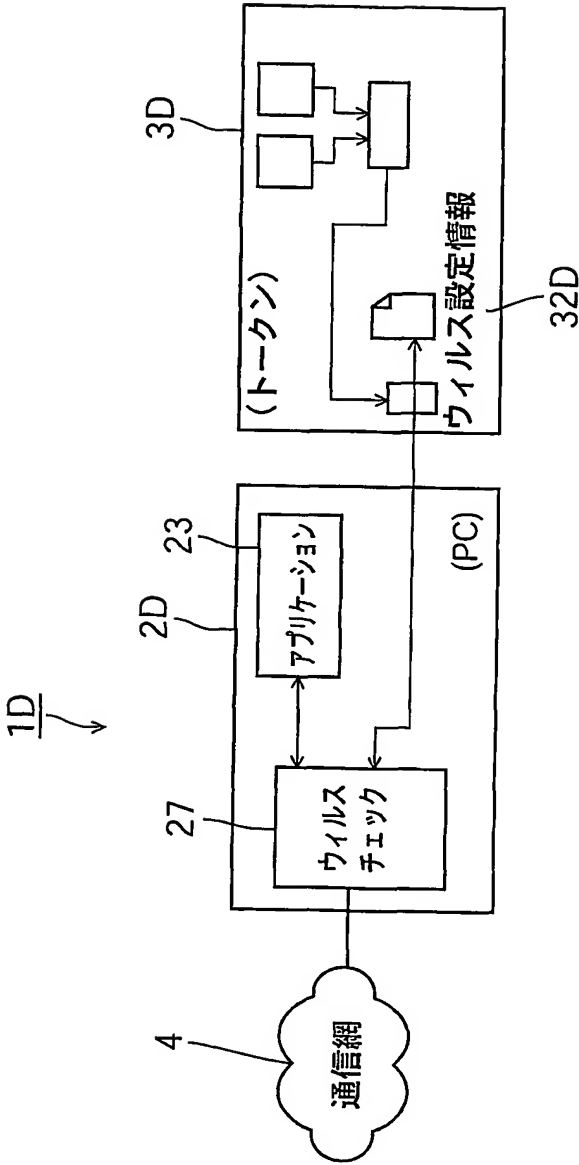
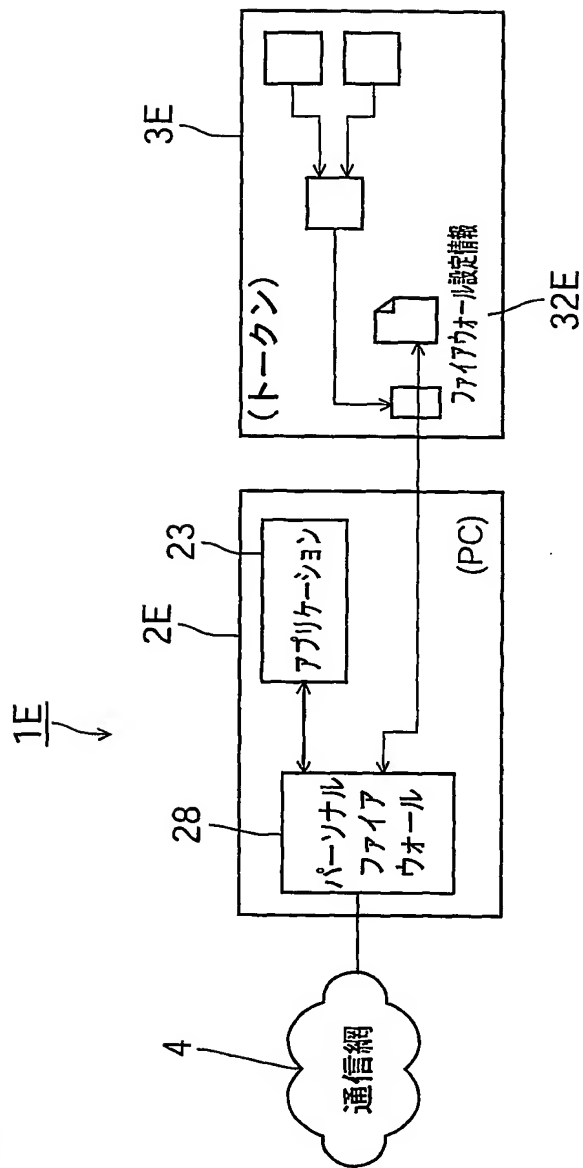


図8



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/12943

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H04L12/56, H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> H04L12/56, H04L12/22, G06F13/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2003  
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Ken KOMATSUBARA, "NTT-ken ga VPN-kino o PC Card ni Kotonaru Machine ya OS de Yoi ni Riyo Kano", Nikkei Internet Technology, Vol.52, 22 October, 2001 (22.10.01), page 17; full text; all drawings	1-4, 6, 7 5, 8-10
X Y	SMC Smart Modem Card Smart Modem Card no Tokucho, [online], NTT Information Sharing Platform Laboratories, 2001, [14 January, 2003 (14.01.03), retrieval date], Internet, <URL: http://www2.pflab.ecl.ntt.co.jp/index/kenkyu/html/18/smc_c/gaiyou.htm>, full text; all drawings	1-4, 6, 7 5, 8-10

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
14 January, 2003 (14.01.03)

Date of mailing of the international search report  
28 January, 2003 (28.01.03)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/12943

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 00/36566 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.), 22 June, 2000 (22.06.00), Page 3, lines 1 to 10; page 3, lines 32 to 34; page 6, lines 16 to 22 & JP 2002-532997 A Page 9, lines 18 to 28; page 10, lines 12 to 14; page 14, lines 1 to 8 & EP 1057145 A1 & CN 1297553 A & KR 2001086236 A & TW 472217 A & US 2002/124176 A1	5,8-10

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl. H04L 12/56, H04L 12/22

## B. 調査を行った分野

## 調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl. H04L 12/56, H04L 12/22, G06F 13/00,  
H04L 9/00

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
 日本国公開実用新案公報 1971-2003年  
 日本国登録実用新案公報 1994-2003年  
 日本国実用新案登録公報 1996-2003年

## 国際調査で利用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	小松原健, NTT研がVPN機能をPCカードに異なるマシンやOSで容易に利用可能, 日経インターネットテクノロジー, 第52号, 2001. 10. 22, 第17頁, 全文, 全図	1-4, 6, 7 5, 8-10
X Y	SMC スマートモデムカード スマートモデムカードの特徴, [online], NTT情報流通プラットフォーム研究所, 2001, [2003年1月14日検索], インターネット, <URL: http://www2.pflab.ecl.ntt.co.jp/index/kenkyu/html/18/smc_c/gaiyou.htm>, 全文, 全図	1-4, 6, 7 5, 8-10

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
 「O」 口頭による開示、使用、展示等に言及する文献  
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」 同一パテントファミリー文献

国際調査を完了した日

14. 01. 03

国際調査報告の発送日

28.01.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)  
 郵便番号100-8915  
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

江嶋 清仁



5X

2947

電話番号 03-3581-1101 内線 3594

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	WO 00/36566 A1 (KONINKLIJKE PHIL IPS ELECTRONICS N. V. ) 2000. 06. 2 2, 第3頁第1-10行, 第3頁第32-34行, 第6頁第16- 22行 & JP 2002-532997 A (第9頁第18-28行, 第10頁第12-14行, 第14頁第1-8行) & EP 1057145 A1 & CN 1297553 A & KR 2001086236 A & TW 472217 A & US 2002/124176 A1	5, 8-10